

## R E M A R K S

Applicant has carefully considered the Office Action of April 5, 2005 rejecting all of the claims. The present response is intended to fully address all points of objection raised by the Examiner, and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the application are respectfully requested.

Claims 1 and 22 have been currently amended. Claim 15 has been previously amended. Claims 2 to 11, 16 to 21, and 23 to 24 have been previously deleted. Therefore, claims 1, 12-15 and 22 remain in the case.

In a post-final interview with the Examiner, conducted by telephone on 31 May 2005, a proposed amendment was suggested to the independent claims relating to a public key algorithm.

The Examiner noted that this amendment may overcome the cited reference, but there may be a need for a further search.

It is respectfully put forward by the Applicant that there is no reason for a further search and consideration. The context of the invention was originally framed in relation to the rise of the Internet data highway, which has dramatically increased the need for secure data transmission, per page 1, 1<sup>st</sup> paragraph, lines 1 to 9.

Therefore, it is clear that the surrounding technology of the inventive method and device was always secure data transmission related to Internet communication. Applicant believes that the Examiner should have taken this into account with the initial search.

The present invention discloses a secure data entry peripheral device configured as a secure keyboard device in a computer system adapted for Internet communication.

The secure keyboard device comprises a public key algorithm for insuring secure data transmission in a secure Internet communication format enabling dynamic key exchange.

The inventive secure data entry peripheral device encryption technique is embedded within the keyboard device itself without an external communication link, and the encryption technique is not carried out separately on the computer unit or devices attached by wires or add-on software programs. Thus, each transmission of data from the peripheral device is already encrypted, giving it a high level of security with its initial transmission from the device.

Claim 1 has been amended to overcome the objection made by the Examiner, wherein the word 'siad' is replaced by the word 'said'. Therefore, claim 1 is deemed to be patentable, and dependent claims 12 to 15 are deemed to be patentable as being based thereon.

The Examiner has rejected claims 1, 12 to 15 and 22 under Sec. 112 as being indefinite for failing to particularly point out and distinctly claim the limitation of the phrase "encoding/decoding" as well as the phrase "encrypting/decrypting".

Therefore, claim 1 has been amended so that the phrase "encoding/decoding", will now be understood to mean "encoding and decoding".

Accordingly, claim 22 has been amended so that the phrase "encrypting/decrypting", will now be understood to mean "encrypting and decrypting".

This is sufficiently supported by the specification at page 11, 3<sup>rd</sup> paragraph, lines 1 and 2, which defines the secure keyboard as a device that can provide, with a different encryption key, the decryption of data sent to it by the computer for purposes of authentication.

The Examiner has rejected claims 1 to 6, 12 to 15 and 22 under Sec. 102(b) as being anticipated by Clark.

The preamble of claims 1 and 22 have been amended to more clearly emphasize the surrounding technology of the inventive device, as a secure data entry peripheral device adapted for Internet communication.

Furthermore, claims 1 and 22 have been amended to more clearly define the novelty and non-obviousness of the inventive device and method, comprising a public key algorithm for encoding and decoding data information in a secure Internet communication format enabling dynamic exchange of system encryption keys.

The amendments made herein to claims 1 and 22 are sufficiently supported by the specification at page 11, 3<sup>rd</sup> paragraph, lines 5 to 8, which describe the fact that numbers and data values within the inventive encryption program are encrypted by various methods, including a dynamic exchange of system encryption keys and public key technology, such as RSA algorithms, Diffie-Hellman, etc.

In addition, page 1, 2<sup>nd</sup> paragraph, as well as page 13, 1<sup>st</sup> paragraph, lines 1 and 2, mentions that this security level is adapted for Internet communication, requiring secure data transmission for purchases and transactions via the Internet.

However, the Clark patent suggests nothing regarding a computer system adapted for Internet communication.

The system described by the Clark patent largely relates to typical transactions within closed systems, e.g. ATM, banks, lottery, that employ encryption methods such as a PIN code, as described in the background, per col. 1, lines 39-48. This is additionally stated in the description, at col. 2, lines 30-36 and at col. 8, lines 19-29.

However, encryption methods, such as a PIN code, may only provide a low security level within closed systems. Therefore, the encryption methods to which Clark relates are completely inadequate for encoding and decoding data information in a secure Internet communication format known today.

Furthermore, the Clark patent relates to encryption circuitry that is integrated into a keyboard associated with a PC, such that confidential data is transmitted to the PC and manipulated by the PC in an encrypted form, per col. 2, lines 42-48.

However, Clark does not disclose that the encryption circuitry is integrated into a keyboard in a secure Internet communication format.

In contrast, according to the present invention, the inventive secure keyboard device in a computer system is adapted for Internet communication, wherein the communication is between the remote server and the secure keyboard device. The computer system (such as a PC) functions only as a physical path between the secure keyboard device and the Internet network. Therefore, data transmitted via the computer system is already encrypted and there is no need for further encryption.

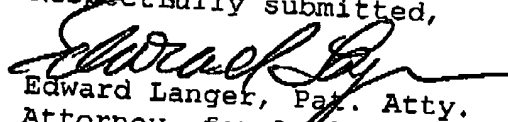
Therefore, claims 1 to 6, 12 to 15 and 22 are not anticipated under Sec. 102(b).

As stated in the decision in *In Re Marshall*, 198 USPQ 344 (1978), "To constitute an anticipation, all material elements recited in a claim must be found in one unit of prior art...". Since the Clark reference neither 1) identically describes the invention, nor 2) enables one skilled in the art to practice it, Applicant deems the 102(b) rejection improper, and respectfully requests that it be withdrawn.

It is respectfully put forward by the Applicant that there is no reason to consider the present invention as being anticipated by Clark, since Clark does not disclose a secure data entry peripheral device configured as a secure keyboard device adapted for Internet communication, wherein the controller means comprises a public key algorithm for encoding and decoding data information in a secure Internet communication format enabling dynamic exchange of system encryption keys. Actually the Clark patent is not an option for the modern internet communication which the only way to construct a reliable secure connection is by a key exchanges mechanism.

In view of the foregoing remarks, all of the claims in the application are deemed to be allowable. Further reconsideration and allowance of the application is respectfully requested at an early date.

Respectfully submitted,

  
Edward Langer, Pat. Atty.  
Attorney for Applicant  
Reg. No. 30, 564

Shiboleth, Yisraeli, Roberts and Zisman LLP  
350 Fifth Ave., 60<sup>th</sup> Floor  
New York, NY 10118  
212-244-4111 telephone  
212-563-7108 fax

324230/1